UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,127	01/14/2000	Alan Dowd	105.176US1	7964

21186 7590 12/19/2002

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER
MAKHDOOM, SAMARINA

ART UNIT	PAPER NUMBER
2123	

DATE MAILED: 12/19/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/483,127	Applicant(s) DOWD ET AL.	
	Examiner Samarina Makhdoom	Art Unit 2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/14/2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2. Claims 1-8, 10-37 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al., U.S. Patent No. 6,088,804.

As per Claims 1 and 18, Hill et al. disclose a security modeling system comprising:

a network configuration module having network configuration data (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that configure the devices and protocols of the network);

and a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that answer 'what if' questions or analyze the network for different network configurations in a network defining database),

wherein the simulator includes a network vulnerabilities database (See Col. 6, lines 14-22 for a database of attacks which include the severity or network vulnerability associated with each attack).

As per Claims 2 and 11, Hill et al. disclose a network vulnerabilities database includes network vulnerability, attack and exploitation data (See Figure 3, and text in Col 7, lines 47 et Seq. for a database with network attack, vulnerability or severity level, and attack or exploitation data).

As per Claims 3 and 12, Hill et al. disclose a network configuration data and the network vulnerability, attack and exploitation data are stored in database tables and the data is processable by a computer (See Figure 3, and text in Col 7, lines 47 et Seq. for a database with network attack, vulnerability or severity level, and attack or exploitation data as part of a computer system therefore the data information is processed by the computer).

As per Claims 4 and 19, Hill et al. disclose a network configuration module comprises network configuration data output by a network configuration discovery tool (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that analyze the network for different network configurations in a network defining database).

As per Claims 5, 13, 22, and 31 Hill et al. disclose a simulator includes a graphical user interface (See Figure 7, and text in Col. 8, line 62 et Seq. for a network status display that is a graphical user interface).

As per Claims 6 and 15, Hill et al. disclose a simulator includes a means for receiving the network vulnerability, attack and exploitation data (See Col. 2, lines 45-60 for a network system that evolves (or receives feedback data) with evolving threats such as attacks and network exploitation such as viruses).

As per Claims 7 and 17, Hill et al. disclose a simulator includes a defender and an attacker user interface (See Col. 5, lines 38-45 where the attacks are entered by an operator therefore the system includes a user interface).

As per Claims 8 and 16, Hill et al. disclose a security modeling system is portable (See Col. 4, lines 5-10 that the security system may be incorporated into an existing network, therefore, the system can run on different networks and is portable).

As per Claim 10, Hill et al. disclose a security modeling system comprising:

a network configuration module having network configuration data (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that configure the devices and protocols of the network);

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that answer 'what if' questions or analyze the network for different network configurations in a network defining database),

wherein the simulator includes a network vulnerabilities database (See Col. 6, lines 14-22 for a database of attacks which include the severity or network vulnerability associated with each attack);

and a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information (See Col. 4, lines 42-53 for security agents that are associated with nodes or resources and have information about what events are occurring at that resource such as port scans and penetration attempts. Therefore, the security agent of Hill et al. functions as a mission objective module).

As per Claims 14 and 30, Hill et al. disclose the critical resource information includes goals, expectations and constraints for simulating the network (See Col 4, lines11-41 for information on simulating the network such hierarchy and links that set the goals, expectations and limits or constraints of the network).

As per Claim 20, Hill et al. disclose the network configuration includes receiving a data file, which includes a configuration of the computer network (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that configure the devices and protocols of the network, therefore configuration data is received by the Hill et al. network).

As per Claim 21, Hill et al. disclose the network includes:

receiving mission objectives (See Col. 4, lines 42-53 for security agents that are associated with nodes or resources and have information about what events are occurring at that resource such as port scans and penetration attempts. Therefore, the security agent of Hill et al. functions as a mission objective module);

storing the objectives (See Col. 4, lines 42-53 for security agents that are associated with nodes or resources and have information about what events are occurring at that resource such as port scans and penetration attempts. Therefore, the security agent of Hill et al. functions as a mission objective module);

and simulating the network based on the network configuration and mission objectives (See Col. 8, lines 62 et Seq. for a network status display that displays the network status based on the current security event situation or current mission).

As per Claim 23, Hill et al. disclose the simulation includes dynamically interacting with an attacker (See Col. 7, line 64 et Seq. for the attack response process that dynamically interacts

with the attacker by detecting and repulsing the security events at the nodes. Also the SOM processor is notified of the outcome of defending the attacks through one of the security agents).

As per Claims 24-25, Hill et al. disclose the simulation includes dynamically interacting in real time with the security modeling system (See Col. 7, line 64 et Seq. for the attack response process that dynamically interacts with the attacker by detecting and repulsing the security events at the nodes. Also the SOM processor is notified of the outcome of defending the attacks through one of the security agents).

As per Claims 26 and 32, Hill et al. disclose the determining of vulnerabilities includes computing security results, wherein the security results include a security score (See Figure 3, where 61 attack severity is given a security score or level such as low, medium, or high).

As per Claim 27, Hill et al. disclose the determining of vulnerabilities of the simulated network includes updating the vulnerabilities database when vulnerabilities are detected (See Col. 9, lines 35-45 where the security system predicts patterns for subsequent attacks and updates the attack signatures thereby evolving with the threats).

As per Claim 28, Hill et al. disclose the method of opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information (See Col. 8, lines 62 et Seq. for the network status display that has the status information of the network);

receiving mission objectives (See Col. 4, lines 42-53 for security agents that are associated with nodes or resources and have information about what events are occurring at that

resource such as port scans and penetration attempts. Therefore, the security agent of Hill et al. functions as a mission objective module);

receiving commands from a network attacker (See Col. 7, lines 55-67 for receiving information on system security attacks);

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components (See Col. 8, lines 5-67 for simulating the network based on attack information and vulnerability or attack severity data based on the network hardware and software status display information);

and responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network (See Col. 8, lines 50-58 for the mitigation list that is a list of recommended actions that may be taken to mitigate an attack).

As per Claim 29, Hill et al. disclose the network further includes receiving commands from a defender and determining results based on the defender commands (See Col. 7, lines 64 et Seq. for the response process from the network defender beginning with task 82 that detects and repulses the security event. The security agent in task 88 notifies the SOM processor of the attack thereby determining the results based on the defender's commands).

As per Claim 33, Hill et al. disclose the receiving commands includes receiving attack actions, which include commands that simulate service functionality, commands that change

services or nodes, and commands that exploit vulnerabilities (See Col. 8, lines 62 et Seq. for the attack status information list and attack signature logs that issue commands such as telling the SOM process or to instruct nodes not to respond to external communication or force new passwords).

As per Claim 34, Hill et al. disclose the security modeling system for simulating objective networks comprising:

a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data (See Figure 3, for a database of simulated attack information or vulnerability or severity table, See Col. 8, lines 62 et Seq. for network status display information or network configuration data and attack signature log files);

and a graphical user interface which operates with the simulator to allow input and output to clients (See Figure 7, and text in Col. 8, line 62 et Seq. for a network status display that is a graphical user interface).

As per Claims 35-37, Hill et al. disclose the mission objectives tables include mission tables, mission files tables and mission services tables (See Figure 3, for a database of simulated attack information or vulnerability table, See Col. 8, lines 62 et Seq. for network status display information or network configuration data and attack signature log files. Also see Col. 4, lines 62 et Seq. for the input and correlation of data used to train the SOM processor to respond to attacks. This data would need to be stored in a database, table, or list).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al. in view of Perlman, U.S. Patent No. 5,558,339.

As per Claim 9, Hill et al. disclose computer simulator comprising:

a network configuration module having network configuration data (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that configure the devices and protocols of the network);

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration (See Col. 1, line 59 to Col. 2, line 11 for network modeling tools that answer 'what if' questions or analyze the network for different network configurations in a network defining database),

wherein the simulator includes a network vulnerabilities database (See Col. 6, lines 14-22 for a database of attacks which include the severity or network vulnerability associated with each attack),

and wherein the simulator includes a graphical user interface (See Figure 7, and text in Col. 8, line 62 et Seq. for a network status display that is a graphical user interface).

Hill et al. disclose a security simulator with a user interface but not a security game.

Perlman discloses a game to be played over a secure network (See abstract) in the same field of endeavor.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the simulator of Hill et al. with the game of Perlman because it would make Hill et al's simulator easier to use and more enjoyable.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shwed et al. U.S. Patent No. 5,835,726 disclose a novel system for controlling the inbound and outbound data packet flow in a computer network.

Shostack et al., U.S. Patent No. 6,298,445 disclose enhancements to computer security software.

Woodward, U.S. Patent No. 4,942,573 discloses a parallel network simulator with a time multiplexed bus.

Boebert et al., U.S. Patent No. 5,864,683 disclose a system and method for secure transfer of data between networks.

Maloney et al., U.S. Patent 6,253,337 disclose the analysis of a system that resides on a network.

Diep, U.S. Patent No. 6,370,648 disclose detecting harmful or illegal intrusions on a computer network with statistical analysis.

Ghosh, S.; Robinson, P. "A framework for investigating security attacks in ATM networks," IEEE Military Communications Conference Proceedings. MILCOM 1999. Volume: 1 Pages: 724 –728.

Smith, R.N.; Bhattacharya, S. "A protocol and simulation for distributed communicating firewalls," Proceedings of the Twenty-Third Annual International Computer Software and Applications Conference, COMPSAC '99. Pages: 74 –79.

Samfat, D.; Devernay, V.; Bonnet, C. "A GSM simulation platform for intrusion detection," IEEE International Conference on Communications, ICC '95 Seattle, 'Gateway to Globalization', Volume: 2 , Pages: 766 –770.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samarina Makhdoom whose telephone number is 703-305-7209. The examiner can normally be reached on Full Time on Tuesday, Thursday, Friday, and Sunday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kevin J. Teska can be reached on 703-305-9704. The fax phone numbers for the

organization where this application or proceeding is assigned are 703-305-0040 for regular communications and 703-305-0040 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

SM
December 12, 2002